REMARKS

Claim Status

Applicants acknowledge, with appreciation, the Examiner's indication that claims 2, 3, 4 and 5 contain allowable subject matter. Claims 1-5, 10 and 11 are currently pending, with claims 1, 10 and 11 being in independent form. Claims 6-9 have been canceled. Claims 1-5, 10 and 11 have been amended. The amendments to claims 2-5 are merely cosmetic or clarifying in nature. No new matter has been added. Reconsideration of the application, as herein amended, is respectfully requested.

Information Disclosure Statement

An Information Disclosure Statement (IDS) is being filed concurrently herewith. Entry and acknowledgment that the IDS and the references cited therein have been entered and considered is requested.

Overview of the Office Action

The Specification has been objected to based on a minor informality. Withdrawal of this objection is in order, as explained below.

Claims 6 and 10 stand rejected under 35 U.S.C. §101 as directed to non-statutory subject matter. Claim 6 has been canceled. Therefore, the rejection with respect to claim 6 is moot. Withdrawal of the rejection with respect to claim 10 is in order, as also explained below.

Claims 1, 5, 10 and 11 stand rejected under 35 U.S.C. §112, second paragraph, as indefinite for failure to particularly point out and claim the subject matter which applicants regard as the invention. Withdrawal of this rejection is also in order, as explained below.

Claims 1, 10 and 11 stand rejected under 35 U.S.C. §103(a) as unpatentable over "Group Signature Schemes and Payment Systems Based on the Discrete Logarithm Problem", Swiss Federal Institute of Technology Zürich, 1998 ("*Camenisch*") in view of U.S. Patent No. 6,896,044 ("*Inada*"), and further in view of "Efficient and Secure Member Deletion in Group Signature Schemes", Center for Information Security Technologies (CIST), Korea University, Seoul Korea, pgs. 150-161, 2001 ("*Kim*").

Claims 6-9 stand rejected under 35 U.S.C. §103(a) as unpatentable over *Camenisch* in view of *Inada*. In view of the cancellation of claims 6-9, this rejection is moot.

Applicants have carefully considered the Examiner's rejections, and the comments provided in support thereof. For the following reasons, applicants respectfully assert that all claims now pending in the present application are patentable over the cited art.

Amendments Addressing Section 112 issue and Formalities

The Examiner has stated that "[t]he 'item 20' in Fig. 1 is used for three different elements described in the specification" 'calculation means 20' *(pars. 0079-0080), 'server 20' (pars. 0082-0083, 0086, and 0089)*, and the 'memory space 20' *(par. 0091)*".

In response to this objection, applicants point out that paragraph [0080] of U.S. Publication No. 2005/0169461 (i.e., the instant published application) explains that "[a] trusted authority, such as a physical person, a moral person, or a national or international agency, maintains calculation means 20 that are shown in FIG. 3 in the form of a server. The calculation means 20 are connected by first communications means 22 to a communications network 23 which may be a public network such as the Internet or a private network such as a local area network (LAN). That is, the calculation means 20 is the server 20". Therefore, the use of reference numeral 20 for both the calculation means and the server is appropriate.

With respect to the "memory space 20", described at paragraph [0091] of the instant published application, applicants have amended the specification as originally filed to now recite "The calculation means 25 of the smart card 21_1 connect to the memory space of the server 20 or the associated storage means 36 in which a directory is stored via the personal computer 28 and the network 23". Support for this amendment may be found, for example, at paragraph [0086] of the instant published application or the paragraph at pg. 15, line 36 to pg. 16, line 7 of the originally filed specification. No new matter has been added. Withdrawal of the objection to the specification is in order.

The Examiner stated that claims 1, 6, 10 and 11 recite "'*n members*;' however, 'n' is not explicitly defined". In response to this rejection, claims 1, 10 and 11 have been amended in a self-explanatory manner. Withdrawal of this rejection is also in order.

Descriptive Summary of the Prior Art

Camenisch discloses a cryptographic method of anonymously signing a message by a member of a group of members (see Chap. 4, paragraphs 4.1.2 and 4.3.4). In particular, *Camenisch* (Chap. 4, Introduction) explains that "[a] group signature scheme allows a member of group to sign messages anonymously on behalf of the group. In the case of a later dispute a designated group manager can revoke the anonymity and identify the originator of the signature".

Inada discloses "a system for allowing only an arbitrary member in a group to decrypt and write a signature by use of a group key which is allowed to be used by only the group member" (see col. 1, lines 9-12).

Kim discloses a group signature scheme that allows deletion of members from the group, as well as the security requirements (see Sec. 2).

Summary of the Subject Matter Disclosed in the Specification

The following descriptive details are based on the specification. They are provided only for the convenience of the Examiner as part of the discussion presented herein, and are not intended to argue limitations which are unclaimed.

The specification discloses a cryptographic method of anonymously signing a message by a member and preventing revoked members from signing messages.

A signature is created when an attempt is made to initially update the common private key copy of a member. An anonymous signature of the message is then calculated using a group private key, and an additional signature of a combination comprising the message and the anonymous signature is calculated using the copy of the member's common private key.

Any member that is revoked from the group will no longer be permitted to correctly sign a message because the revoked member is no longer capable of calculating a correct additional signature of the combination comprising the message and the anonymous signature because the revoked member will not possess the updated common private key. This common private key is updated by a trusted authority on each revocation of a member from the group, and is encrypted with as many symmetrical secret keys as there are non-revoked members. Consequently, a revoked member cannot decrypt any of the different encrypted forms of the common private key that were obtained using the symmetrical secret key of this revoked member.

Patentability of the Independent Claims under 35 U.S.C. §101

The Examiner (at pg. 3 of the Office Action) asserts, with respect to claim 10, that:

> although the preamble of the claim recites "cryptographic system," the body of the claim may be directed to software implementation since they do not recite any elements of hardware; "calculation means," "asymmetric keys," and "symmetric keys," could be implemented by software by one of ordinary skill in the art at the time the invention was made. Therefore, the claimed

subject matter does not belong to any of the four statutory subject matters set forth above.

Applicants disagree.

The preamble of independent claim 10 has been amended to recite "A cryptographic system for anonymously signing a digital message, the system comprising". Independent claim 10 has been also amended to recite "first calculation means ... and ... a smart card associated with each member in the group, each smart card comprising...." The smart card is described, for example, at pg. 14, lines 20-21 of the instant specification. As further described at pg. 15, lines 30-34 of the instant specification, "[t]he smart card 21_1 stores in its storage means 24 the common private key 31, the member's group private key 33_1 and the secret key 34_1 assigned to the member during the interaction between the trusted authority and the member". The skilled person would readily appreciate that this component comprises hardware that forms a component of the claimed cryptographic system – itself hardware.

In view of the foregoing, applicants contend that independent claim 10 is directed, *inter alia*, to hardware components and, therefore, this claim is directed to statutory subject matter. Withdrawal of the rejection is accordingly deemed to be in order.

Patentability of the Independent Claims Under 35 U.S.C. §103(a)

Independent claim 1 has been amended to clarify the salient aspects of the disclosed invention. Thus, independent claim 1 now recites, *inter alia*, "a tenth step of calculating, at the calculation means of the signing member, an additional signature of a combination comprising the message and the anonymous signature using the up-to-date common private key of the signing member". Independent claims 10 and 11 have been amended to correspondingly recite at least this feature. No new matter has been added.

The Examiner (at pg. 6 of the Office Action) asserts that:

> Camenisch discloses ... a tenth step in which the member's calculation means (24) calculate (operation 13) an additional signature of the combination comprising the message and the anonymous signature using the member's common private key (31) *(pages 102-103 and 107-108; sections 5.4.3, 5.4.4, 5.5.3 and 5.5.4; signing messages and opening signature).*

Applicants disagree.

Camenisch (Chap. 4, paragraph 4.3.4) explains that "[t]he unlinkability of two or more group signatures originated from the same members follows from the fact that signatures of the type SPK_{11} and SPK_{10} are unlinkable and from the fact that the y_i's are probabilistically encrypted. This guarantees anonymity". *Camenisch* (Chap. 4, paragraph 4.1.2) additionally explains that a method is provided in which "the manager cannot falsely accuse members (even if she is also a group member). Furthermore, we also present the first generalized group signature scheme. In both schemes, the functionality of opening signatures can be shared among several entities such that the identity of a signer can still be revealed efficiently by them. Both schemes allow the addition (or removal) of group members after the initial step". *Camenisch* thus teaches a cryptographic method of anonymously signing a message by a member of a group comprising a plurality of n members.

Camenisch, however, fails to teach or suggest step 10 as now recited in amended independent method claim 1. Chapter 5 of *Camenisch* is directed to *group signature schemes for large groups*. In particular, Section 5.4 describes the basic group signature scheme. Paragraph 5.4.3 of *Camenisch* explains how messages are signed, and paragraph 5.4.4 states the conclusion that "signatures are anonymous and unlinkable". There is however no teaching or suggestion in these paragraphs as to exactly what might constitute the "additional signature" provided by independent claims 1, 10 and 11. That is, there is nothing in paragraphs 5.4.3 and 5.4.4 of *Camenisch* with respect to calculating an additional signature using the common private key of a

member. *Camenisch* thus fails to teach or suggest "an additional signature of a combination comprising the message and the anonymous signature using the up-to-date common private key of the signing member", as now recited in amended independent claim 1.

The Examiner cites *Inada* to remedy the failure of *Camenisch* to teach or suggest the claimed fifth, seventh and eighth steps of independent claim 1. Applicant disagrees, however, that any combination of *Camenisch* and *Inada* achieves the recited subject matter of independent claim 1, or the subject matter correspondingly recited in independent claims 10 and 11. *Inada* fails to teach or suggest anything with respect to calculating an additional signature using the common private key of a member. What *Inada* does disclose is a system for providing group signatures.

In particular, *Inada* teaches an asymmetric pair of keys that are shared by the members of the group, i.e., public/private keys (P_G/S_G). The common private key S_G of *Inada* must be acquired by all valid members of the group (which does not include revoked members). *Inada* teaches a method in which the acquisition of the common private key S_G by group members is accomplished via ciphering of the common private key. The ciphering of *Inada* differs, however, from the ciphering associated with the claimed invention.

Inada (col. 3, lines 4-8) explains that "the common key which has been encrypted...is sent to a group/member"). *Inada* teaches that each time a member is deleted, the following steps are performed: (i) a private key of the encrypted group lock $C_G(S_G)$ is calculated (see step 106 of FIG. 8), (ii) a new public key $P_{Mi}(C_G)$ is calculated (see step 106 of FIG. 8), and (iii) the new public key $P_{Mi}(C_G)$ is communicated to each non-revoked member.

The claimed invention, on the other hand, provides a method that has considerable practical advantages over the method of *Inada*. *Inada* teaches a method that requires two encryption steps, i.e. (i) and (ii) above. In the first step, the common private key S_G is encrypted

using the common group key C_G. The second step requires the use of public keys P_{Mi} of a respective member Mi to encrypt the common key C_G (see col. 13, lines 48-45). In contrast, step 7 of amended independent claim 1, i.e., the "seventh step of encrypting, at the first calculation means of the trusted authority, the up-to-date common private key using each of the symmetrical secret keys to obtain as many encrypted forms of the up-to-date common private key as there are non-revoked members", requires only a single encryption of the common private key 31 using each of the symmetrical secret keys 34_i of non-revoked members. The trusted authority of *Inada*, on the other hand, is required to perform for each remaining group member an additional encrypting step, whereas in applicants' claimed method and apparatus only a single encrypting step is initially performed. Moreover, in the *Inada* method, each member of the group is required to also perform one additional calculation than in Applicants' claimed method to decrypt the common private key S_G (see step 607 of FIG. 14).

In contrast to the method of *Inada*, the claimed invention advantageously eliminates the necessity to inform each non-revoked member that a new common private key S_G has been created or encrypted, i.e., there is no step (iii) of *Inada* in which the new public key $P_{Mi}(C_G)$ must be communicated to each non-revoked member. In the *Inada* method, each non-revoked member is informed of the encryption of the new common private key by sending to each non-revoked member a new $P_{Mi}(C_G)$ value. Such sending of a new $P_{Mi}(C_G)$ value to each member is time consuming and place larges demands on available computational power. In the claimed invention, step 8 – i.e., an eighth step of updating the common private key stored in the storage means of the signing member if one encrypted value of the up-to-date common private key may be decrypted using the symmetrical secret key stored in the storage means of the signing member – is performed to update the common private key only when a member wishes to sign a new message.

The skilled person would have no reason to combine the teachings of *Camenisch* with the teachings of *Inada* to achieve the subject matter of independent claims 1, 10 and 11, absent impermissible hindsight based on applicants' instant disclosure. In the *Camenisch* publication, the word "revocation" is associated with "anonymity". Specifically, the meaning of the word "revocation" in *Camenisch* is evidenced at page 72, lines 3-7 of the *Camenisch* publication. There, *Camenisch* explains that "there is a trusted third party, called the group manager, who can reveal the identity of the originator of a signature in the case of later dispute". *Camenisch* describes this as "opening" a signature or as the revocation of a signer's anonymity – not removal of a member from the group.

The signature "opening" procedure of *Camenisch* differs substantially from the revocation or removal of a group member's inclusion or credentials within the meaning and scope of applicants' claims. In *Camenisch*, the opening procedure is necessary to determine, by testing the identity of the member, who it is that issued a specific signature, i.e., to remove the member's anonymity so as to "reveal the identity of the originator". In contrast, the "revocation" of applicants' claims solves the problem of withdrawing from a member of a group the ability to apply a group anonymous signature each time that the group changes; the claimed invention prevents a previous member of the group who is no longer allowed (revoked) to generate an authorized group signature. Moreover, the old and well-known signature "opening" procedure of *Camenisch* is itself described in the instant specification. As explained at pg. 3, lines 14-19 of the specification, "the addressee may contact the trustee authority, which is able to determine the identity of the signatory from the encrypted identifier accompanying the group anonymous signature. Thus, the trusted authority is able to remove the anonymity at any time". The combination of steps 4 to 10 with steps 1-3 of applicants' independent claim 1 thus provides a solution to a problem that is markedly different from that which is the subject of *Camenisch*.

As explained at pg. 7, lines 5-15 of the instant specification, "the method of the invention adds to the anonymous signature of a message effectuated by a member, an additional signature calculated using a copy, held by the member, of a signature private key that is exactly the same for all the members authorized to sign and unknown to all revoked members. This common private key is updated by the trusted authority each time a member of the group is revoked. The copy held by a member is updated only when the member signs a message anonymously, and this updating is possible only for a non-revoked member". There is nothing in *Camenisch* with respect to the problem of revocation as that term is used in applicants' disclosure and claims. Therefore, the combination of *Camenisch* and *Inada* fails to teach or suggest at least steps 1-5 and steps 7-10 of independent claim 1, which are correspondingly recited in independent claims 10 and 11. In any event, the combination of *Camenisch* and *Inada* fails to achieve independent claims 1, 10 and 11 *at least* because *Inada* fails to provide what *Camenisch* lacks, i.e., calculating an additional signature using the common private key of a group member.

The Examiner cites *Kim* to remedy the acknowledged failure of *Camenisch* and *Inada* to teach or suggest the claimed sixth step of independent claim 1. Applicant disagrees, however, that any combination of *Camenisch*, *Inada* and/or *Kim* achieves the subject matter of independent claim 1, or the subject matter correspondingly recited in independent claims 10 and 11. *Kim* fails to teach or suggest anything with respect to calculating an additional signature using the common private key of a group member.

Kim teaches a method for modifying two keys, i.e., an ownership public key U_M and a renewal public key U_N, each time that a member is deleted (revoked) from a group. *Kim* explains that "to delete the group member G_j the membership manager eliminates public key y_{Gj} from the group public property key U_M and changes a random number" (see pg. 157, Section 4.3). There is no teaching or suggestion, however, in *Kim* with respect to calculating an

additional signature using the common private key of a member, as recited in now amended independent claim 1, and correspondingly recited in now amended independent claims 10 and 11.

The Examiner justifies his proffered combination of *Kim* with *Camensich* and *Inada* by reference to pg. 151, lines 15-16 of *Kim*. However, the skilled person would have no reason to combine the teachings of *Camenisch* and *Inada* with the deletion protocol of *Kim* in the Examiner's proffered manner, absent impermissible hindsight based on applicants' instant disclosure.

Kim explains that "[i]n this paper, we propose a new group signature scheme which allows member deletion and sign-tracing generated by a specific member." However, the text immediately following lines 15-16 on pg. 151 of *Kim* explains that "Our Scheme is based on Camenisch and Michels' group Signature Scheme [4] that adds a member deletion procedure." Moreover, the *Kim* publication is cited in the description of the instant specification. As explained at pg. 5, lines 12-19 of the instant specification, "[t]hat method has the drawback of being specific in application, in that it has proven to be secure only in a particular group signature scheme that corresponds to that described in the paper by J. Camenisch and M. Michels "A Group Signature Scheme With Improved Efficiency", in K. Ohta and D. Pei, editors, Advances In Cryptology – ASIACRYPT '98, Volume 1514 of LNCS, pages 160-174, Springer-Verlag. 1998". As also described at pg. 5, lines 20-24 of the specification, "that method has the disadvantage that it imposes calculations on each member each time that a member joins or leaves the group; these calculations may become frequent if the dynamics of the group are particularly intense." The combination of *Camenisch*, *Inada* and *Kim* thus fail to achieve a system that provides a solution to these drawbacks.

The claimed invention, on the other hand, advantageously eliminates these problems by calculating, at the calculation means of a signing member, an additional signature of a combination comprising the message and an anonymous signature using the up-to-date common private key of the signing member. This common private key is automatically updated by a trusted authority each time that a member of the group is revoked or eliminated. The copy of the private key held by a member is updated only when that member thereafter signs a message anonymously, and this updating is possible only for a non-revoked member of the group. Consequently, a revoked member is always identified and detected since the "additional signature" of the revoked member will be false because the revoked member will not possess an updated private key. The combination of *Camenisch*, *Inada* and *Kim* fails to teach or suggest a system and method that encompasses or permits this advantageous feature and functionality. The combination of *Camenisch*, *Inada* and *Kim* thus fails to achieve the express recitations of independent claims 1, 10 and 11.

By virtue of the above-discussed differences between the recitations of independent claims 1, 10 and 11 and the teachings of *Camenisch* in combination with *Inada* and *Kim*, and the lack of any clear motivation for modifying the reference teachings to achieve applicants' claimed invention, independent claims 1, 10 and 11 are deemed to be patentable over any combination of *Camenisch*, *Inada* and *Kim* under 35 U.S.C. §103.

Dependent Claims

In view of the patentability of independent claims 1, 10 and 11 for the reasons presented above, each of dependent claims 2-5 is respectfully deemed to be patentable therewith over the prior art. Moreover, each of these dependent claims includes features which serve to still further distinguish the claimed invention over the applied art.

Conclusion

Based on all of the above, applicants submit that the present application is now in full and proper condition for allowance. Prompt and favorable action to this effect, and early passage of the application to issue, are once more solicited.

Should the Examiner have any comments, questions, suggestions or objections, the Examiner is respectfully requested to telephone the undersigned to facilitate an early resolution of any outstanding issues.

Respectfully submitted,
COHEN PONTANI LIEBERMAN & PAVANE LLP

By _____

Lance J. Lieberman
Reg. No. 28,437
551 Fifth Avenue, Suite 1210
New York, New York 10176
(212) 687-2770

Dated: October 14, 2008